REMARKS

Claims 7-13, 17-19 and 21-31 are pending.

Claims 7-12, 21-22, 24-25, and 30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6,389,532, hereinafter referred to as Gupta) in view of Hakim et al. (U.S. Patent Pub. No. 2002/0167943, hereinafter referred to as Hakim).

Claims 13, 17-19, 23, 26-29, and 31 are rejected under 35 U.S.C. §103(a) as being unpatentable over Gupta in view of Hakim, and further in view of Gibbs et al. (U.S. Patent No. 6,085,321, hereinafter referred to as Gibbs).

Claims 7, 17, 21, 27, and 30-31 are amended. Claims 8-10, 18-19, and 28-29 are canceled. The features recited in claims 8-10, 18-19, and 28-29 have been incorporated in the respective independent claims 7, 17, 21, 27, and 30-31.

Claims 7, 11-13, 17, 21-27, and 30-31 remain in the case for reconsideration.

The applicant adds no new matter and requests reconsideration in light of the above amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 112

Claims 21-26 are rejected for insufficient antecedent basis in the Office Action mailed February 9, 2007. The applicant amends claim 21 to include proper antecedent basis. Therefore, claim 21 and its dependent claims 22-26 are in condition for allowance in this regard.

Claim Rejections – 35 U.S.C. § 103

Claims 7-12, 21-22, 24-25, and 30 are rejected as being obvious over Gupta in view of Hakim. The applicant disagrees for the reasons that follow.

Claim 7 recites "transmitting the content file when data comprising the content file does not include the restricted data format; and blocking transmission of the content file when data comprising the content file does include the restricted data format." Claims 17, 21, 27, and 30-31 include similar features as in claim 7.

The Examiner acknowledges that Gupta does not teach these features. Office Action, Page 3. The Examiner, however, alleges Hakim teaches transmitting the digital content when the content does not contain the restricted data format (The Examiner has identified Hakim's multimedia information being the restricted data format recited in the claims), "because Hakim filters the multimedia information to prevent sending it." *See* Office Action, page 11,

last paragraph, through page 12, first paragraph.

Hakim teaches "Security to prevent sensitive information from being listened to or filtered is accomplished via the use of a firewall that is capable of filtering multimedia information, specifically voice packets." *See* Hakim [0099]. That is, Hakim uses a firewall to prevent sensitive information, such as multimedia information, from being filtered, such that multimedia information passes through the firewall, while non-multimedia information is blocked. Put yet another way, Hakim transmits multimedia information, while blocking information that is not multimedia. This is in direct contrast from "transmitting the content file when data comprising the content file does not include the restricted data format; and blocking transmission of the content file when data comprising the content file does include the restricted data format" recited in the claims.

In addition, Claim 7 incorporates the features recited in the original claims 8-10, which have been canceled. Claim 7 recites "the restricted data format including at least one of a MP3 data format, a MPEG video data format, and a Word document format." Claims 17, 21, 27, and 30-31 include similar features as in claim 7.

The Examiner has identified Hakim's multimedia information being the restricted data format recited in the claims. But Hakim's multimedia information is specifically voice packets, e.g., voice packets of an international call. *See* Hakim [0099], and [0088]. Hakim does not mention or suggest that its multimedia information may include at least one of a MP3 data format, a MPEG video data format, and a Word document format. Hakim's multimedia information cannot be the restricted data format as claimed.

The Examiner further alleges that it would be obvious to modify Gupta to "provide security to prevent sensitive information, such as audio, to be transmitted." Office Action, Page 4. But there is no such suggestion or motivation to combine the reference teachings.

Gupta teaches a method for using digital signatures to filter packets in a network in order to prevent wasting of network resources associated with unauthorized senders in a multicast context. See Abstract, and Col. 1, lines 56-62. According to Gupta, A malicious user may engage in what is called a denial of service attack to send numerous unauthorized messages to an end host system on the other side of a router or a firewall, which can cause a network bottleneck. *See* Gupta Col. 1, lines 45-55. Gupta does not concern with security to prevent sensitive information from being listened to or filtered. Instead Gupta mainly concerns with unauthorized senders sending packets to cause network bottleneck and waste of network resources. As such, Gupta does not require or benefit from Hakim's firewall to

prevent sensitive information from being listened to or filtered. Accordingly, no such motivation exists to combine these teachings and the combination of Gupta and Hakim is invalid.

Neither Gupta alone nor in combination with Hakim teaches claims 7, 17, 21, 27, and 30-31. Claims 7, 17, 21, 27, and 30-31, as well as their dependent claims are in condition for allowance.

Claim 21 recites "transmitting the content file when the content file includes the digital signature; and blocking transmission of the content file when the content file does not include the digital signature to prevent unauthorized downloading of copyrighted material."

The Examiner alleges that Gupta teaches the above feature, citing Col. 4, lines 12-13. Gupta, however, teaches "A sender signs the packet using the one of the private keys. A router or a firewall then determines the validity of the signature by checking the signature using the public key. If the signature is valid, the router or firewall forwards the packet. Packets having an invalid signature are discarded." *See* Gupta Col. 2, lines 17-21. Specifically, Gupta discloses "Router 104 then determines whether signature 310 is valid by comparing the decrypted fingerprint and the fingerprint 308. If the two values match, the signature is valid. If signature 310 is valid, router 104 forwards the packet in step 720. If signature 310 is not valid, then router 104 discards the packet, in step 722. *See* Gupta Col. 7, lines 19-27, and FIG. 7, steps 718 and 722. In other words, Gupta forwards a packet if the packet has a valid digital signature, and discards the packet if the digital signature is not valid. Put yet another way, Gupta's decision to transmit or discard a packet is based on the validity of the digital signature in the packet, rather than based on the presence of a digital signature in the content file as claimed.

Furthermore, Gupta does not teach preventing unauthorized downloading of copyrighted material as recited in claim 21. Gupta teaches avoiding wasting router bandwidth and resources on processing packets associated with unauthorized senders. *See* Gupta, FIG. 7, steps 706, 710, 718, 722, and Col. 1, lines 56-62. Gupta embeds a digital signature in each packet to prevent unauthorized sending from unauthorized senders. In other words, Gupta's digital signature is not used for protecting copyrighted digital content, but rather used for identifying the unauthorized senders who may cause a network bottleneck. Put yet another way, Gupta prevents unauthorized sending from unauthorized senders regardless of the content of material that are being sent, e.g., copyrighted digital content or otherwise.

Gupta does not teach claim 21, and Hakim does not cure Gupta's deficiencies in Gupta. Claims 21 and its dependent claims 22-26 are allowable.

Claim Rejections – 35 U.S.C. § 103

Claims 13, 17-19, 23, 26-29, and 31 are rejected as being obvious over Gupta in view of Hakim, and further in view of Gibbs. The applicant disagrees for the reasons that follow.

Claim 17 recites "using at least one router configured to log digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the related digital signatures...." Claims 23, 27 and 31 include similar features.

The Examiner alleges that Gibbs teaches the feature of a log record, citing FIG. 4, Ref. 432, and Col. 6, lines 17-26, and Col. 7, lines 56-67. But Gibbs does not teach a record including the related digital signatures.

As shown in Gibbs' FIG. 2, Gibb teaches an authentication log file 200 (also referred to as authentication log file 432 in FIG. 4), which comprises a plurality of exemplary records (204, 208, 212, 216, and 220). Each record of the authentication log file 200 contains three fields: system key number field 230, which points to a corresponding record of the authentication log file 200; system key field 234 that stores the system key 108 of FIG. 1, which is a 256 bit value that is randomly generated by the authenticated message server 100 and used for generating a block of unique digital signatures that is equal in number to the number of bits in the bit vector (e.g., 224); and status field 240, which is a bit vector (e.g., 224) for storing status information about each of the unique digital signatures successfully authenticated by the authenticated message server 100, for example a value of "1" in a bit of the bit vector means that a particular unique digital signature has been used. *See* Gibbs Col. 4, lines 10-65, and Col. 3, lines 50-52. In other words, Gibbs' authentication log file 200 includes the status of the unique digital signature that has been successfully authenticated, rather than the unique digital signature itself. In fact, Gibbs' unique digital signature 132 comprises three parts: a service id 136, a digital signature 144, and a domain name 148. *See* Gibbs, Col. 3, lines 20-30, and FIG. 1. None of the fields in Gibbs' authentication log file 200 includes these three parts of a unique digital signature.

The Examiner further alleges that it would have been obvious to modify Gupta/Hakim in view of Gibbs to keep track of the status information and other information about the creation and authentication of digital signatures.

But neither Gupta nor Hakim requires or benefits from maintaining a log file to keep track of the status information and other information about the creation and authentication of digital signatures. Hakim discloses an Internet calling apparatus and method for placing international toll-free calls. Hakim does not disclose anything about the creation and authentication of digital signatures.

Gupta, on the other hand, teaches a method for using digital signatures to filter packets in a network in order to prevent wasting of network resources associated with unauthorized senders in a multicast context. As it is commonly known in the art, multicast is a form of communication in which a single message is sent to multiple destination at once. *See* Gupta Col. 1, lines 20-25. In order for a multicast packet to reach multiple receivers, the nodes or routers in the network may be required to replicate the multicast packet. This means multicat communication requires a large amount of router bandwidth. In Gupta, a digital signature is created and stored in the header of each multicast packet. *See* Gupta Col.5, lines 30-35, and FIG. 3, box 310. To maintain an authentication log file for the related digital signature in a router would slow down the router performance and tie up the network resources and bandwidth, resulting in a network bottleneck. Thus, maintaining an authentication log file for the related digital signature may contradict the objectives that Gupta aims to accomplish, which is to avoid wasting router bandwidth and resources in a multicast context. *See* Gupta Col.1, lines 57-62.

Gibbs adds nothing to overcome the deficiencies in Gupta and Hakim. Consequently, Gupta and Hakim in view of Gibbs does not render obvious all of the limitations as set forth in claims 17, 23, 27, and 31. Claims 17, 23, 27, and 31, as are the dependent claims, are allowable.

In view of the foregoing amendments and remarks, applicant believes the application should be in condition for allowance. If any questions remain, the Examiner is requested to call the undersigned.

Respectfully submitted,

20575
Customer No.

MARGER JOHNSON & McCOLLOM, P.C.

By _____
Julie L. Reed
Reg. No. 35,349

210 S.W. Morrison Street, Suite 400
Portland, Oregon 97204
Telephone: (503) 222-3613